

BC

(19)



Europäisches Patentamt
European Patent Office
Office européen des brevets



(11)

EP 0 848 872 B1

(12)

EUROPÄISCHE PATENTSCHRIFT

(45) Veröffentlichungstag und Bekanntmachung des Hinweises auf die Patenterteilung:
22.03.2000 Patentblatt 2000/12

(51) Int Cl.7: **H04L 9/32**

(86) Internationale Anmeldenummer:
PCT/EP96/03893

(21) Anmeldenummer: 96931023.4

(87) Internationale Veröffentlichungsnummer:
WO 97/09802 (13.03.1997 Gazette 1997/12)

(22) Anmeldetag: 04.09.1996

(54) **VERFAHREN UND VORRICHTUNG ZUR VERSIEGELUNG VON COMPUTERDATEN**
METHOD AND DEVICE FOR THE SEALING OF COMPUTER DATA
PROCEDE ET DISPOSITIF POUR LE SCELLEMENT DE DONNEES INFORMATIQUES

(84) Benannte Vertragsstaaten:
AT BE CH DE DK ES FI FR GB GR IE IT LI LU MC
NL PT SE

(74) Vertreter: Meyer, Enno (DE)
Weser & Kollegen
Patentanwälte
Radeckestrasse 43
81245 München (DE)

(30) Priorität: 04.09.1995 DE 19532617

(43) Veröffentlichungstag der Anmeldung:
24.06.1998 Patentblatt 1998/26

(56) Entgegenhaltungen:
WO-A-92/03000 DE-A- 4 411 780

(73) Patentinhaber: Timesafe Trustcenter GmbH
90425 Nürnberg (DE)

• ADVANCES IN CRYPTOLOGY - CRYPTO '87.
PROCEEDINGS, SANTA BARBARA, CA, USA,
16-20 AUG. 1987, ISBN 3-540-18796-0, 1988,
BERLIN, WEST GERMANY,
SPRINGER-VERLAG, WEST GERMANY, Seiten
216-222, XP000130206 DAVIDA G I ET AL:
"Arbitration in tamper proof systems. If DES
approximately=RSA then what's the difference
between true signature and arbitrated signature
schemes?"

(72) Erfinder:
• Nissl, Klaus
80999 München (DE)
• Meinhold, Matthias
90425 Nürnberg (DE)
• Günther, Hartmut
90489 Nürnberg (DE)

[Faint, illegible text, likely bleed-through from the reverse side of the page]

[Faint, illegible text, likely bleed-through from the reverse side of the page]

Anmerkung: Innerhalb von neun Monaten nach der Bekanntmachung des Hinweises auf die Erteilung des europäischen Patents kann jedermann beim Europäischen Patentamt gegen das erteilte europäische Patent Einspruch einlegen. Der Einspruch ist schriftlich einzureichen und zu begründen. Er gilt erst als eingelegt, wenn die Einspruchsgebühr entrichtet worden ist. (Art. 99(1) Europäisches Patentübereinkommen).

EP 0 848 872 B1

Beschreibung

[0001] Der elektronische Daten- und Informationsaustausch mittels Computer, Telefax, Telex und anderen entsprechenden Medien hat in den letzten Jahren einen gewaltigen Aufschwung erhalten. Der wachsende Einsatz der EDV auf allen Gebieten steht angesichts der Qualität und der Quantität des verarbeiteten Datenumaterials vor einer völlig neuen Dimension der geforderten Datensicherheit. Dies gilt insbesondere für die Datenfernübertragung (DFÜ), wie tägliche Presseberichte zeigen. Beispiele finden sich in Ärzte-Zeitung 14, Nr. 86, 11.05.95 "Internet ist für sensible Daten nicht geeignet" und PraxisComputer Nr. 10, 10. Februar 1995, S. 15 "Trau' keinem über Fax ...".

[0002] Die Forderung nach Datenversiegelung, Dokumentenechtheit und rechtsverbindlicher Kommunikation wird immer lauter. Es ist eine Frage der Zeit, bis der Gesetzgeber entsprechende Richtlinien erläßt. Der Wortlaut eines entsprechenden Interviews ist in PraxisComputer Nr. 5, 10. August 1995, S. 36 "Knappe Ressourcen besser nutzen", Interview mit Dr. Winfried Schorre und Horst Seehofer, abgedruckt.

[0003] Einige der denkbaren Manipulationsmöglichkeiten werden im folgenden kurz aufgeführt, um die Sachlage zu verdeutlichen.

Beispiel Medizin

[0004] Der Operateur erstellt postoperativ per Diktat, das anschließend von der Schreibkraft in den Computer eingegeben wird, den Operationsbericht. Nachträglich stellt sich heraus, daß der Operateur einen Fehler begangen hat, z.B. aufgrund einer zuvor diagnostizierten Linsentrübung. Entfernung der Augenlinse, allerdings auf der falschen Seite. Nachträglich versucht der Operateur, den präoperativen Befund (Linsentrübung links) zu manipulieren (Linsentrübung rechts), um sich zu entlasten.

Beispiel Finanzen

[0005] Transaktionen mit einem Wechselkurs zum Zeitpunkt t1. Zum Zeitpunkt t2 ist der Kurs gefallen, eine nachträgliche Manipulation soll in betrügerischer Weise den Verlust verhindern.

Beispiel Forschung

[0006] Wer hat eine Erfindung zuerst dokumentiert?

Beispiel Rechtswesen

[0007] Protokollerstellung bei der Beweisaufnahme, bei deren Verwendung vor Gericht Dokumentenechtheit gefordert wird.

Beispiel Datenaustausch

[0008] Der Entlassungsbrief eines Psychiatriepatienten soll per Modem an den Hausarzt gesendet werden. Die Authentizität des Empfängers muß sichergestellt und eine unbefugte Einsichtnahme in die vertraulichen Unterlagen verhindert werden. Siehe auch in PraxisComputer Nr. 6, 15. Oktober 1994, S. 5 "Schweigepflicht und Datennetze".

[0009] Die Physikalisch Technische Bundesanstalt in Braunschweig sendet die durch eine Cäsiumuhr ermittelte Uhrzeit mittels Funkwellen von Mainflingen aus. Das Signal kann im Umkreis von 1500 - 2000 km empfangen werden. Näheres unter ELV-Journal 6/94, S. 27 ff "DCF Empfangstechnik".

[0010] Die Empfängermodule für Funkuhrsignale besitzen ein hohes technisches Niveau (wie in Design&Elektronik 10, 16.05.95, Kennziffer 242 "Industrie-Uhren im Atomzeitalter" näher erläutert) und liefern jede Minute die komplette Datum-/Uhrzeitinformation, im folgenden als Normalzeit bezeichnet.

[0011] Auch im Ausland existieren Zeitzeichensignale wie zum Beispiel MSF (England) und WWV (USA), ferner ist das Zeitsignal in GPS (globales Positionsbestimmungssystem, s.u.) enthalten.

[0012] Seit es Informationen gibt, besteht der Wunsch, diese durch Verschlüsselung vor dem allgemeinen Zugriff zu schützen. Die Sicherheit des eingesetzten Schlüssels korreliert mit der Güte des Schlüsselalgorithmus.

[0013] Zur Geheimhaltung vertraulicher Daten stehen verschiedene Verschlüsselungsverfahren zur Verfügung, die entsprechend dem Aufwand eine mehr oder weniger große Datensicherheit bieten. Prinzipiell unterscheidet man zwischen symmetrischen (Kryptoverfahren nach Feal, DES u.a.) und asymmetrischen Verfahren (RSA, PGP u.a.).

[0014] Verschiedene Unternehmungen in Richtung Dokumentenechtheit und rechtsverbindlicher Kommunikation haben bislang keine befriedigende Lösung erbracht. Die Gleichstellung der digitalen Signatur mit der eigenhändigen Unterschrift ist Gegenstand intensiver Forschung, wie in ct Magazin 1995, Heft 6, S. 46 "Krypto-Neid" und in Design&Elektronik, 14/15, 18.07.95, Kennziffer 212 "Single-Chip-Controller für Kryptokarten" ausgeführt. Gegenüber der alleinigen Verschlüsselung bietet die digitale Signatur vielfältige Vorteile (Glade, A., Reimer, H., Struiß, B. "Digitale Signatur und sicherheitssensitive Anwendungen, Wiesbaden 1995).

[0015] Die nachträgliche Manipulierbarkeit von EDV-Daten stellt ein bislang ungelöstes Problem dar. Zum Dokument im juristischen Sinne wird eine Datei erst durch ihren Ausdruck, der mit Datum und Unterschrift versehen werden muß. Angesichts der Datenfülle und der Geschwindigkeit ihrer Erzeugung und Vernichtung (Datenturnover) stößt dieses Verfahren an die Grenzen des Machbaren.

[0016] Der wachsende Datenaustausch per Compu-

ter, Telefax und anderen Medien sowie die permanent steigende Anzahl von Vernetzungen auf nationaler und internationaler Ebene (Internet u.a., siehe auch in der Ärzte-Zeitung 14, Nr. 86, 11.05.95 "Internet ist für sensible Daten nicht geeignet") erfordern adäquate Maßnahmen zur Datensicherheit. Näheres in Praxis-Computer Nr. 1, 10. Februar 1995, S. 15 "Trau' keinem über Fax..." und c't Magazin 1994, Heft 8, S. 230 ff.: "Datenschlösser, Grundlagen der Kryptologie") WO-A-92/03 000 offenbart ein System zum Zeitstempeln eines digitalen Dokuments. Dabei präpariert ein Autor ein digitales Dokument und sendet es in einer ersten Ausführungsform zu einer Zeitstempelinstitution (Authority, TSA). Dort wird das Dokument zeitgestempelt, d.h. es werden dem Dokument digitale Daten zugefügt, die die Zeit repräsentieren, und die Institution fügt noch ihre Signatur zu, um beispielsweise die Richtigkeit oder Echtheit der Zeitstempelung zu dokumentieren. Dann wird das mit der Zeitstempelung und der Signatur versehene Dokument an den Autor zurückgesendet, der damit später einen Beweis der Existenz des ursprünglichen Dokuments führen kann. Um eine spätere Manipulation an dem Dokument zu verhindern, kann das Dokument vor dem Senden an die TSA mittels beispielsweise einer Hashfunktion komprimiert werden, wobei die Hashkompression anstelle des Dokuments bei der Institution zeitgestempelt und signiert wird. Eine zweite Ausführungsform unterscheidet sich von der ersten dadurch, daß anstelle der Institution ein Netz oder eine "Welt" von Autoren verwendet wird, die sich gegenseitig nach einem Zufallsprinzip die Zeitstempelung und Signierung auf die versendeten Dokumente erteilen. Die Institution TSA bzw. die Autorenwelt benutzt als Zeit die "Computer clock time", d.h. die manipulierbare interne Uhr des mit der Zeitstempelung befaßten Computers.

[0017] Der Artikel von Davida et al.: "Arbitration in Tamper Proof Systems", Advances in Cryptologie-Crypto 87 Proceedings, Santa Barbara, CA, USA, 16-20. Aug. 1987, ISBN 3-540-18796-0, 1988, Berlin, West-Germany, Springer Verlag, Seiten 216-222, beschreibt verschiedene Verfahren zum Erzeugen von manipulationssicheren Systemen, so unter anderem digitale Signatursysteme, Systeme mit öffentlichen Schlüsseln und Notarsysteme, die eine Zeitstempelung beinhalten. So wird eine Nachricht unter Verwendung einer Vorrichtung verschlüsselt. Dabei wird in der Vorrichtung eine Nachrichtennummer mc und ein Zeitstempel ts an die Nachricht angehängt und verschlüsselt. Aus dem Ergebnis, d.h. der Nachricht plus der Nummer mc plus dem Zeitstempel ts , wird eine verschlüsselte Hashfunktion h generiert. Allerdings wird keine Aussage über die verwendete Zeit getroffen.

[0018] Nachteilig bei den obigen bekannten Verfahren und Systemen ist die Tatsache, daß keines der Verfahren eine sichere Zeit gewährleisten kann, so daß eine Manipulationsmöglichkeit hinsichtlich der verwendeten Zeit nicht gewährleistet ist.

[0019] Der Erfindung liegt daher die Aufgabe zugrun-

de, ein Verfahren und eine Vorrichtung zum Erstellen eines Zeitstempels bzw. zum Versiegeln von digitalen Daten zu schaffen, wobei die für die Zeitstempelung benötigte Zeit eine geringe Manipulationsmöglichkeit aufweist.

[0020] Die Aufgabe wird durch die Merkmale der Verfahrensansprüche 1. und 2. sowie der Vorrichtungsansprüche 11 und 12 gelöst. Bevorzugte Ausgestaltungen der Erfindung sind Gegenstand der Unteransprüche.

[0021] Das hier beschriebene Verfahren und die Vorrichtung bewirken, daß der Zugriff auf die so versiegelten Daten in der Regel verwehrt bleibt und stellen damit einen wesentlichen Schritt in Richtung Dokumentenechtheit und rechtsverbindlicher Kommunikation dar (s. Fig. 1 Datenflußschema).

[0022] Für den Datentransport bedeutet dies, daß die Authentizität von Sender und Empfänger gewährleistet und eine unbefugte Einsicht in die versandten Daten durch die gleichzeitige Verschlüsselung verhindert wird.

[0023] Das Verfahren und die Vorrichtung zur Versiegelung von Computerdaten mittels Kombination aus Normalzeiteinbindung, Authentisierung und Verschlüsselung schützt die so versiegelten Daten vor unberechtigtem Zugriff bzw. Manipulation, sowohl im stationären EDV-Bereich (Ausführungsbeispiel PC-Einsteckkarte) als auch bei der Datenfernübertragung (Ausführungsbeispiel Zusatzplatine). Siehe, Fig. 2: Vorrichtung zur Datenversiegelung.

[0024] Auf der PC-Ebene wird zur Nachrüstung eine Einsteckkarte, für die DFÜ-Geräte eine Zusatzplatine, favorisiert. Selbstverständlich ist es ein Bestreben der Technik, derartige Schaltungen zu miniaturisieren und auf möglichst kleinem Raum zusammenzufassen. Vor allem bei Neugeräten läßt sich stückzahlabhängig auch eine anwenderspezifische IC- (ASIC)-Lösung realisieren. Eine Ankopplung der erfindungsgemäßen Vorrichtung an den PC (d.h. Computer allgemein) kann auch über eine beliebige Schnittstelle (seriell, parallel, PCM-CIA Adapter) erfolgen.

[0025] Die Komponenten der Vorrichtung und des Verfahrens zeigt Fig. 3

[0026] Die Vorrichtung besteht aus elektronischen Bausteinen, die folgende Aufgaben zu erfüllen haben:

- Signalauswertung
- Signalüberprüfung
- Bereitstellung der Identifikationsnummer der Vorrichtung
- Verschlüsselung des empfangenen Signals
- Manipulationskontrolle

Vorhandene Sender:

[0027] Der Sender stellt die Datums- und Uhrzeitinformation bereit. Neben den Zeitzeichensendern kommen auch andere Signalträger wie Satellit, TV-Kabel, Telefon, TV-Sender u.a. in Frage. Außerdem kann sogenannten Providern (z.B. Telekom) die Möglichkeit zur Si-

gnalvergabe bzw. Einbindung eingeräumt werden.

Eigens konstruierte Sender

[0028] Ein eigens konstruierter Sender erhöht die Datensicherheit durch folgende Faktoren:

1. Bereitstellung der Normalzeit in verschlüsselter Form;
2. Variabilität des Sendezeitpunkts;
3. Durchmischung von echter und falscher Information;
4. Sender-Empfängersynchronisation mit begrenzter Gültigkeitsdauer;
5. Mischung der Information von 1-4;
6. Bidirektionales Signal zur Signalübermittlung.

[0029] Die Beschaffenheit des Empfängers hängt von der des Senders ab. Prinzipiell können Funk- und Kabelsignale empfangen werden. Eine entsprechende Logik wertet die empfangenen Signale aus.

[0030] Die Überprüfung der Echtheit geschieht bei dem Funkuhrsignal mangels spezieller zusätzlicher Signale über das Aufwärtszählen des Zeitimpulses, d. h. bei etwaiger Manipulation werden datumsältere Eingaben als das zuletzt abgefragte unverfälschte Datumszeitsignal als Manipulation erkannt. Zusätzlich wird das empfangene Signal mit einer internen Uhr (RTC, Real Time Clock) abgeglichen, wobei Zeitdifferenzen außerhalb eines Kontrollbereiches auf Manipulation hindeuten.

[0031] Die Authentisierung erfolgt über ein Gerät und/oder ein Verfahren, daß die Identität des Senders bzw. des Empfängers einer Nachricht zweifelsfrei festlegt.

Die elektronische Signatur ist derzeit Gegenstand der Forschung (siehe in Design&Elektronik 14/15, 18.07.95, Kennziffer 212 "Single-Chip-Controller für Kryptokarten"). Es eignen sich auch andere Geräte und Verfahren (Kartenleser, Fingerprint-Reader, und Transpondersysteme wie in Design&Elektronik, Kennziffer 283 "Berührungslose Identifikation" beschrieben, u.ä.) zum Nachweis der Authentisierung.

[0032] Die Modifikation des Zeitsignals geschieht mittels Hardware (GAL, PAL und/oder andere Hardware-Verschlüsselungsverfahren wie den Clipper-Chip, der in c't Magazin 1994, Heft 8, S. 24 "Die NSA und der Clipper-Chip" erläutert ist) und/oder mittels Software (Verschlüsselungsalgorithmus; z.B. nach dem RSA-Verfahren; näheres dazu in c't Magazin 1994, Heft 8, S. 230 ff. "Datenschlösser, Grundlagen der Kryptologie". Eine Entschlüsselung kann nur von der Person erfolgen, die den Schlüssel zu der Modifikationslogik besitzt.

[0033] Zur Verhütung einer mechanischen Manipulation werden der Chip bzw. die entsprechenden Komponenten der Einsteckkarte eingegossen und mit einer elektromechanischen Koppelungstechnik versehen, sodaß ein nachträgliches Auslesen von Microprozessor-Elementen erschwert wird. Wie aus Fig. 5 hervor-

geht, hat der Kontakt der Schirmung 1 und 2 das Lösen der programmierten Bauteile zur Folge, sog. Blackbox-Lösung.

[0034] Eine Datenmanipulation wird durch die Paritätsprüfung und andere mathematische und/oder Hardware-Prüfverfahren erkannt. Die Sicherheit steigt mit der Komplexität der Prüfverfahren.

[0035] In Amerika haben unabhängige Einrichtungen für den Datenschutz sogenannte "Trust Center" eingerichtet, um als außenstehende dritte Partei eine Vertrauensfunktion im Datenschutz zu übernehmen. Dies betrifft die Ver- und Entschlüsselung, die Vergabe und das Aufbewahren von Schlüsseln sowie die Kooperation mit Providern und entsprechenden Notariaten zur neutralen Beglaubigung von Kommunikationsschlüsseln, u.ä. Näheres findet sich in Praxis Computer Nr. 2, 10. März 95, S. 16/17. "Mit Chipkarten ist vieles möglich".

[0036] Ein Dokument enthält neben der Identifikation (z.B. Unterschrift), dem Datum und ggf der Zeit auch den Ort der Dokumentenerstellung. Über Satellitenortung (GPS, globales Positionsbestimmungssystem) läßt sich dieser Ort hinreichend identifizieren und in das Dokument genauso einbinden wie z.B. die Normalzeit.

[0037] Wird die Vorrichtung als eine PC-Einsteckkarte ausgeführt, so übernimmt das Funkuhrsignal DCF 77 der Physikalisch-Technischen Bundesanstalt in Braunschweig die Rolle des Senders. Empfänger für Zeitsignale gibt es in verschiedenen Ausführungen (Größe, Empfangscharakteristik). Das empfangene Signal wird demoduliert und verstärkt als ein 100 ms bzw. ein 200 ms Impuls pro Sekunde an die PC-Einsteckkarte zur Auswertung weitergegeben. Ein Microcontroller auf der Einsteckkarte setzt die empfangenen Signalimpulse in eine Zeitinformation um und speichert über eine spezielle Logik, die individuell auf jede Einsteckkarte zugeschnitten ist, die zuletzt empfangene Zeit ab. Die Validierung des DCF-77 Signals zeigt Fig. 7.

[0038] Jede Einsteckkarte ist mit einer individuellen Identifikationsnummer versehen. Hard- und Software verwenden diese Nummer zur Maschinenidentifizierung. Die Bausteine für den Empfang, die Authentisierung und Verschlüsselung brauchen, wie das Ausführungsbeispiel Einsteckkarte am PC in Fig. 6 zeigt, nicht notwendigerweise alle auf der Karte selbst angeordnet zu sein.

[0039] Das von der Originaldatei mittels eines Signaturverfahrens (z.B. MD5, Message Digest 5 von Ron Rivest, u.ä.) erzeugte Signal wird mit einem Header (Information über die beteiligten Größen wie Betriebssystemversion, Dateigröße, u.ä.) versehen und mit einem definierten Teil der Originaldatei selbst zu einem Block geformt, der im vorliegenden Fall eine Größe von 4kByte einnimmt (sogenannter 4kBlock).

[0040] Die Microcontroller-Software greift auf das Zeitsignal zu, baut es in den 4kBlock ein, verschlüsselt diesen in der Blackbox und hängt die zeitgestempelte digitale Signatur an die Originaldatei an. Optional kann diese auch separat gespeichert oder zusammen mit der

Originaldatei erneut verschlüsselt werden. (s. Fig. 8).

[0041] Die Entschlüsselung kann nur über den Schlüsselinhaber erfolgen. Dabei wird eine Überprüfung auf nachträgliche Manipulation durch die Signaturüberprüfung durchgeführt.

[0042] Wird die erfindungsgemäße Vorrichtung als Zusatzkarte ausgeführt, so entsprechen die Voraussetzungen für Sender und Empfänger der Realisierung der Vorrichtung als PC-Einsteckkarte (s.o.).

[0043] Im Bereich der DFÜ kommt neben der Dokumentenechtheit der Datensicherung beim Transport eine entscheidende Rolle zu. Vor dem Versand werden die Daten unter Einbindung des Zeitsignals wie beschrieben verschlüsselt. Ver- und Entschlüsselung erfolgen durch Logik-Bausteine, die entsprechend den Randbedingungen der DFÜ-Geräte auf kleinstem Raum integriert sein müssen. Die Verschlüsselungs-Software wird z.B. im EPROM abgelegt, die Verschlüsselungs-Hardware kann zum Beispiel aus einem Clipper-Chip bestehen.

[0044] Neben den o.a. Sicherheitsvorkehrungen schafft das Zeitsignal durch die Festlegung des Send- und Empfangszeitpunkts wahrer und falscher Information weitere Hürden gegen unbefugte Einsichtnahme und/oder Manipulation.

[0045] Eine bevorzugte Ausführungsform ist nachfolgend anhand der beigefügten Zeichnungen beschrieben, in denen

Fig. 1 ein Datenflußschema der Kommunikation einer versiegelten Datei zeigt,

Fig. 2 ein Schemabild einer erfindungsgemäßen Vorrichtung zur Datenversiegelung zeigt,

Fig. 3 die Komponenten der Vorrichtung nach Fig. 2 zeigt,

Fig. 4 mögliche Sender zur Distribution des verwendeten Zeitsignals zeigt,

Fig. 5 eine Schutzvorrichtung gegen unbefugtes Auslesen der programmierten Bauteile der erfindungsgemäßen Vorrichtung zeigt,

Fig. 6 ein Schemabild des erfindungsgemäßen Verfahrens zeigt, wobei die erfindungsgemäße Vorrichtung alsinsteckkarte eines PCs realisiert ist,

Fig. 7 ein Blockdiagramm der Validierung eines externen Zeitsignals, beispielsweise eines DCF77 Signals, sowie der nachfolgenden Aktualisierung der Echtzeituhr zeigt,

Fig. 8 ein Blockdiagramm der Einbindung der Normalzeit beim Verschlüsseln zeigt, und

Fig. 9 ein Schemabild des Verfahrens und der Vor-

richtung zur Versiegelung von Computerdaten zeigt.

[0046] Fig. 1 zeigt das Datenflußschema einer Datei, die senderseitig verschlüsselt, übertragen und empfangenseitig wieder entschlüsselt wird, wobei zur Verschlüsselung der Daten ein Signal eingebunden wird, das die Normalzeit einer externen Quelle und einen Authentisierungscode enthält. Auf der Senderseite liegt eine Datei des Inhalts abc beispielsweise in einem PC, einem Fax, Telex, Handy oder dergleichen vor. Diese Datei kann über eine Transportebene, beispielsweise Datenfernübertragung (DFÜ) zur Empfängerseite übertragen werden. In diesem Fall ist der Inhalt der Datei manipulierbar. Die Empfängerseite umfaßt gleiche Komponenten wie die Senderseite, nämlich PC, Fax, Telex, Handy, oder dergleichen. Um nachträgliche Manipulationen der Datei ausschließen zu können und damit eine Dokumentenechtheit zu erzielen, wird die senderseitige Datei des Inhalts abc einer Verschlüsselung unterzogen, wobei in die Verschlüsselung validiert eine Normalzeit (extern) und eine Identifikation eingebunden wird. Die so verschlüsselte Datei mit einem nicht lesbaren Inhalt wird über die Transportebene zum Empfänger übertragen. Empfängerseitig wird die übertragene, verschlüsselte Datei durch einen Schlüsselbesitzer entschlüsselt, wobei eine Manipulationsüberprüfung und eine Authentisierungskontrolle stattfindet. Anschließend liegt die Datei wieder in der lesbaren Form mit dem Inhalt abc vor.

[0047] Fig. 2 zeigt ein Diagramm möglicher Ausführungsformen der erfindungsgemäßen Vorrichtung zur Versiegelung von Computerdaten. Im Fall einer stationären Verwendung der Vorrichtung, beispielsweise in einem PC, einem Notebook oder dergleichen, kann die Vorrichtung in der Form einer Einsteckkarte ausgeführt werden, falls das stationäre Gerät nachgerüstet wird. Im Fall eines Neugerätes oder einer Erstausrüstung kann die erfindungsgemäße Vorrichtung durch einen integrierten Schaltkreis, beispielsweise durch ein ASIC, realisiert werden. Wird die erfindungsgemäße Vorrichtung nichtstationär, d.h. in der Datenfernübertragung, beispielsweise in einem Fax, einem Modem oder dergleichen, verwendet, so kann im Fall einer Nachrüstung dies beispielsweise durch eine Zusatzplatine erfolgen. Bei einem Neugerät wird die Vorrichtung wie im stationären Fall durch einen integrierten Schaltkreis, beispielsweise einem ASIC, realisiert.

[0048] Fig. 3 zeigt ein schematisches Strukturdiagramm der erfindungsgemäßen Vorrichtung, bestehend aus den übergeordneten Komponenten Empfänger, Authentisierung und Codierer.

[0049] Der Empfänger empfängt Datum- und Uhrzeitinformation. Weiterhin ist es möglich eine Ortsinformation, die beispielsweise aus einem GPS-Signal stammen kann, ebenfalls einzubinden. Diese Information wird decodiert, wobei in der vorliegenden Ausführungsform zur Verdeutlichung beispielhaft ein Zeitsignaldeco-

der angegeben ist. Als Sender der Datum-, Zeit- und/oder Ortsinformation kommen die im vorangegangenen bereits aufgeführten Quellen einschließlich eines eigens zu diesem Zweck konstruierten Senders in Betracht.

[0050] Die Authentisierung legt die Identität des Senders bzw. Empfängers der Nachricht/Datei fest. Dies kann beispielsweise mittels eines Kartenlesers erfolgen. Ferner kann die Authentisierung mittels eines Identitätsverfahrens, wie einer elektronischen Signatur, erfolgen.

[0051] Die Verschlüsselung der Vorrichtung kann über eine entsprechende Hardware, beispielsweise einem Clipperchip, oder einer geeigneten Software, d. h. einem entsprechenden Verschlüsselungsalgorithmus, erfolgen.

[0052] Fig. 4 zeigt eine nicht vollständige Übersicht über mögliche Sender eines geeigneten Zeitsignals. Das notwendige Zeitsignal kann über Funk, beispielsweise als DCF77-Signal der Physikalisch-Technischen Bundesanstalt Braunschweig, oder über Satellit gesendet werden. Eine Übertragung des Zeitsignals über Kabel innerhalb eines TV-Signals oder Telefonsignals ist ebenfalls möglich.

[0053] Fig. 5 zeigt eine Schutzvorrichtung gegen unbefugtes Auslesen oder Manipulieren der programmierten Bauteile einer erfindungsgemäßen Vorrichtung. Die dargestellte sog. Blackbox-Lösung umfaßt zwei als erste und zweite Schirmung ausgebildete Schutzgitter, die die erfindungsgemäße Vorrichtung umgeben, wobei die auf einer Platine angeordneten elektronischen Bauteile und die Schirmungen in einer Vergußmasse eingegossen sind. Ferner ist ein Akkumulator in der Vorrichtung angeordnet, dessen Potential mit den Schirmungen und den programmierten Bauteilen so verbunden ist, daß eine Kontaktierung (Kurzschluß) der beiden Schirmungen miteinander, beispielsweise ein Löschen oder Zerstören der verbundenen Bauteile zur Folge hätte.

[0054] Fig. 6 zeigt eine Ausführung des erfindungsgemäßen Verfahrens bzw. der Vorrichtung als Einsteckkarte in einem PC und die notwendigen Funktionsteile. Ein Funkursender sendet beispielsweise (Bundesrepublik Deutschland) die Normalzeit als DCF77-Signal.

[0055] Ein geeigneter Funkhorempfänger wandelt diese Signale in ein serielles Taktsignal, das in die als PC-Karte realisierte erfindungsgemäße Vorrichtung gegeben wird. Die PC-Einsteckkarte umfaßt einen Microcontroller, ein EPROM, ein EEPROM, Logikschaltungen, beispielsweise GALs, PALs, ASICs oder dergleichen, einen Codierer und einen Bustreiber. Weiter wird über einen Kartenleser eine entsprechende Signatur eingegeben. Mittels einer Software und der Einsteckkarte wird in dem PC die Datei des Inhalts "abc" verschlüsselt, zeitgestempelt und signiert, so daß sich die zu übertragende Datei mit dem entsprechend verschlüsselten Inhalt ergibt.

[0056] Fig. 7 zeigt die Validierung des empfangenen Zeitsignals in dem Microcontroller der Fig. 6. Der Emp-

fängerbauteil liefert ein DCF77-Signal tocF an den Microcontroller. Das EEPROM der Vorrichtung enthält das zuletzt gültige Zeitsignal t_E , wobei die Bedingung $t_{\text{DCF}} > t_E$ erfüllt sein muß. Eine in der erfindungsgemäßen Vorrichtung angeordnete Echtzeituhr, die als eigenständiger Baustein oder mittels des Microcontrollers realisiert sein kann, enthält die aktuelle Zeit t_A mit einer Toleranz T , die beispielsweise 1 sec/Monat betragen kann. Es wird der Vergleich $t_{\text{DCF}} - t_A < |T| \cdot (t_A - t_E)$ durchgeführt. Ist der Vergleich positiv, so wird das DCF77-Signal zur Zeitstempelung verwendet und die Echtzeit aktualisiert.

[0057] Fig. 8 zeigt schematisch die Einbindung der Normalzeit beim Verschlüsseln. Von einer Originaldatei "demo.txt" wird ein Signal mittels eines Signaturverfahrens erzeugt und mit einem Header versehen. Mit einem definierten Teil der Originaldatei wird daraus ein sog. 4kByte Block "4kblock.sta" erzeugt. In der Blackbox greift der Microcontroller auf das Zeitsignal DCF77 (oder GPS) zu und führt die in der Fig. 7 beschriebene Validierung des DCF77-Signals durch. Der Vorgang ist auf n -Versuche begrenzt. Das validierte Zeitsignal wird in den 4kByte Block eingebaut und in der Blackbox verschlüsselt. Der verschlüsselte 4kByte Block "4kblock.tst", d. h. die sog. zeitgestempelte digitale Signatur, wird mittels einer Software und über den PC-Bus an die Originaldatei "demo.txt" angehängt. Optional kann die Kombination der Originaldatei "demo.txt" und der Signatur "4kblock.tst" separat gespeichert oder zusammen erneut zu einer Datei "demo.tsc" verschlüsselt werden. Weitere Ein-/Ausgänge der Blackbox sind Motherboardaktivierung, Chipkarten-Leser/Schreiber und Transponder.

[0058] Fig. 9 zeigt einen Gesamtüberblick über das Verfahren und die Vorrichtung zur Versiegelung von Computerdaten, sowohl für den "stationären" Betrieb als auch für die "DFÜ"-Anwendung. Die Normalzeit (und gegebenenfalls weitere Informationen) wird mittels eines Zeitsenders oder Kabels einem Send-PC oder Send-DFÜ, z. B. Faxgerät, zugeführt, die die Codierung/Decodierung einer entsprechenden Information (Datei) durchführen. Mittels einer Datenfernübertragung wird die verschlüsselte Datei übertragen (gestrichelte Linien bedeuten ein codiertes DFÜ-Signal). Der jeweilige Send-PC, bzw. das Sender-Fax, ist mit einem entsprechenden Empfangs-PC bzw. Empfangs-Fax über einen entsprechenden DFÜ-Weg verbunden. Die Send-/Empfangsfunktion kann gegebenenfalls vertauscht sein. Sowohl sende- als auch empfangsseitig kann eine Dekodierung, eine Archivierung oder ein Ausdruck erfolgen, falls eine Berechtigung vorliegt.

Patentansprüche

1. Verfahren zum Erstellen eines Zeitstempels für digitale Daten, das die folgenden Schritte aufweist:

- a) Empfangen und Auswerten eines externen Funk- oder Kabelsignals einer externen Zeitquelle, aus dem sich die Normalzeit t_{DCF} ableiten läßt,
- b) Vergleichen der in a) ermittelten Normalzeit t_{DCF} mit einem internen aktuellen Zeitsignal t_A einer internen Uhr,
- c) Zeitstempeln der digitalen Daten, falls die Zeitdifferenz zwischen internem und externem Zeitsignal innerhalb eines vorgegebenen Toleranzbereichs liegt,

- wobei das zuletzt gültige Normalzeitsignal t_E der Ungleichung

$t_{DCF} > t_E$ genügen muß, und

wobei für den Vergleich der aktuellen externen Normalzeit t_{DCF} mit der internen aktuellen Zeit t_A die folgende Ungleichung gelten muß:

$$t_{DCF} - t_A < IT \cdot (t_A - t_E),$$

wobei T die Toleranz der internen Uhr bedeutet.

2. Verfahren zum Versiegeln digitaler Daten, das die folgenden Schritte aufweist:

- a) Empfangen und Auswerten eines externen Funk- oder Kabelsignals einer externen Zeitquelle, aus dem sich die Normalzeit t_{DCF} ableiten läßt,
- b) Vergleichen der in a) ermittelten Normalzeit t_{DCF} mit einem internen aktuellen Zeitsignal t_A einer internen Uhr,
- c) Zeitstempeln der digitalen Daten, falls die Zeitdifferenz zwischen internem und externem Zeitsignal innerhalb eines vorgegebenen Toleranzbereichs liegt,

- wobei das zuletzt gültige Normalzeitsignal t_E der Ungleichung

$$t_{DCF} > t_E$$

genügen muß, und

- wobei für den Vergleich der aktuellen externen Normalzeit t_{DCF} mit der internen aktuellen Zeit t_A die folgende Ungleichung gelten muß:

$$t_{DCF} - t_A < IT \cdot (t_A - t_E),$$

- wobei T die Toleranz der internen Uhr bedeutet,
- d) Verschlüsseln der zeitgestempelten digitalen Daten.

3. Verfahren nach Anspruch 2, dadurch gekennzeichnet, daß ein Signal der zeitgestempelten digitalen Daten erstellt wird, wobei das Signal zeitgestempelt und anschließend verschlüsselt wird.

4. Verfahren nach einem der vorangegangenen Ansprüche, dadurch gekennzeichnet, daß als externes Funk- oder Kabelsignal das Funkuhrsignal DCF77 der Physikalisch-Technischen Bundesanstalt oder das Funkuhrsignal eines anderen Zeit-senders verwendet wird.

5. Verfahren nach einem der Ansprüche 1-3, dadurch gekennzeichnet, daß das externe Funk- oder Kabelsignal von einem unabhängigen Sender erfolgt, wobei das externe Funk- oder Kabelsignal einen Authentisierungscode enthält, der den Sender hinreichend identifiziert.

6. Verfahren nach Anspruch 5, dadurch gekennzeichnet, daß das externe Funk- oder Kabelsignal in verschlüsselter Form gesendet wird.

7. Verfahren nach Anspruch 5 oder 6, dadurch gekennzeichnet, daß das externe Funk- oder Kabelsignal zu einem Zeitpunkt gesendet oder empfangen wird, der selbst Teil der Verschlüsselung ist.

8. Verfahren nach einem der Ansprüche 5-7, dadurch gekennzeichnet, daß das externe Funk- oder Kabelsignal wahre und falsche Informationen enthält.

9. Verfahren nach einem der vorangegangenen Ansprüche, dadurch gekennzeichnet, daß das externe Funk- oder Kabelsignal Informationen enthält, aus denen sich der Empfangsort bestimmen läßt.

10. Verfahren nach einem der vorangegangenen Ansprüche, dadurch gekennzeichnet, daß das externe Funk- oder Kabelsignal ein GPS-Signal ist.

11. Vorrichtung zum Erstellen eines Zeitstempels für digitale Daten, die aufweist:

- einen Empfänger zum Empfangen und Auswerten eines externen Funk- oder Kabelsignals einer externen Zeitquelle, aus dem sich die Normalzeit t_{DCF} ableiten läßt,
- eine interne Uhr zum Erzeugen eines internen Zeitsignals t_A ,
- einen Vergleichszum Vergleich der ermit-

- tellten externen Normalzeit t_{DCF} mit der internen Zeit t_A ,
 - einen Speicher, der ein zuletzt gültiges Normalzeitsignal t_E enthält, und
 - ein Mittel zum Zeitstempeln der digitalen Daten falls die Zeitdifferenz zwischen internem und externem Normalzeitsignal innerhalb eines vorgegebenen Toleranzbereichs liegt,
- wobei das zuletzt gültige Normalzeitsignal t_E der
- Ungleichung

$$t_{DCF} > t_E$$

- genügen muß, und
- wobei für den Vergleich der aktuellen externen Normalzeit t_{DCF} mit der internen aktuellen Zeit t_A die folgende Ungleichung gelten muß:

$$t_{DCF} - t_A \leq T * (t_A - t_E)$$

- wobei T die Toleranz der internen Uhr bedeutet.

12. Vorrichtung zum Versiegeln digitaler Daten, die aufweist:

- einen Empfänger zum Empfangen und Auswerten eines externen Funk- oder Kabelsignals einer externen Zeitquelle, aus dem sich die Normalzeit t_{DCF} ableiten läßt,
 - eine interne Uhr zum Erzeugen eines internen Zeitsignals t_A ,
 - einen Vergleichler zum Vergleichen der ermittelten externen Normalzeit t_{DCF} mit der internen Zeit t_A ,
 - einen Speicher, der ein zuletzt gültiges Normalzeitsignal t_E enthält,
 - ein Mittel zum Zeitstempeln der digitalen Daten falls die Zeitdifferenz zwischen internem und externem Normalzeitsignal innerhalb eines vorgegebenen Toleranzbereichs liegt,
- wobei das zuletzt gültige Normalzeitsignal t_E der Ungleichung

$$t_{DCF} > t_E$$

- genügen muß, und
- wobei für den Vergleich der aktuellen externen Normalzeit t_{DCF} mit der internen aktuellen Zeit t_A die folgende Ungleichung gelten muß:

$$t_{DCF} - t_A \leq T * (t_A - t_E)$$

- wobei T die Toleranz der internen Uhr bedeutet,

und

- ein Mittel zum Verschlüsseln der zeitgestempelten digitalen Daten.

13. Vorrichtung nach einem der Ansprüche 11 oder 12, dadurch gekennzeichnet, daß nach einer positiven Auswertung des Vergleichs die Normalzeit t_{DCF} als das zuletzt gültige Zeitsignal t_E im Speicher gespeichert wird und die interne Echtzeituhr aktualisiert wird.

14. Vorrichtung nach Anspruch 12 oder 13, dadurch gekennzeichnet, daß die Vorrichtung ein Mittel zum Erstellen eines Signals der zeitzustempelnden digitalen Daten aufweist, wobei das Signal zeitgestempelt und verschlüsselt wird.

15. Vorrichtung nach einem der Ansprüche 11 bis 14, dadurch gekennzeichnet, daß die Vorrichtung eine Authentisierungsvorrichtung aufweist.

16. Vorrichtung nach einem der Ansprüche 11 bis 15, dadurch gekennzeichnet, daß die Vorrichtung mit einer Identifikationsnummer versehen ist, die in den Verschlüsselungsvorgang eingebunden ist.

17. Vorrichtung nach einem der Ansprüche 11 bis 16, dadurch gekennzeichnet, daß die Signalverarbeitung in der Vorrichtung durch Mikroprozessorbau- steine durchgeführt wird.

18. Vorrichtung nach einem der Ansprüche 11 bis 17, dadurch gekennzeichnet, daß die Vorrichtung gegen ein Heruntertakten geschützt ist.

19. Vorrichtung nach einem der Ansprüche 11 bis 18, dadurch gekennzeichnet, daß die Vorrichtung mit ihren Bauelementen eingegossen und mit einer elektromechanischen Kopplungstechnik versehen ist.

20. Vorrichtung nach einem der Ansprüche 11 bis 19, dadurch gekennzeichnet, daß die Vorrichtung sich auf einer Computerhauptplatine oder innerhalb eines DFÜ-tauglichen Geräts befindet.

21. Vorrichtung nach einem der Ansprüche 11 bis 19, dadurch gekennzeichnet, daß die Vorrichtung als PC-Einsteckkarte oder Zusatzplatine realisiert ist.

Claims

1. A method of preparing a time stamp for digital data comprising the following steps:

- a) Receiving and evaluating an external broadcast or cable signal from an external time

source from which the standard time t_{DCF} can be derived,

b) Comparing the standard time t_{DCF} obtained in a) with an internal actual time signal t_A from an internal clock,

c) Time-stamping the digital data if the difference between the internal and the external time signal is within a preset tolerance range,

wherein the latest valid standard time signal t_E must satisfy the inequality

$$t_{DCF} > t_E,$$

and

wherein the following inequality must apply for comparison of the actual external standard time t_{DCF} with the actual internal time t_A :

$$t_{DCF} - t_A < IT * (t_A - t_E),$$

wherein T denotes the tolerance of the internal clock.

2. A method of sealing digital data comprising the following steps:

a) Receiving and evaluating an external broadcast or cable signal from an external time source from which the standard time t_{DCF} can be derived,

b) Comparing the standard time t_{DCF} obtained in a) with an internal actual time signal t_A from an internal clock,

c) Time-stamping the digital data if the difference between the internal and the external time signal is within a preset tolerance range,

wherein the latest valid standard time signal t_E must satisfy the inequality

$$t_{DCF} > t_E,$$

and

wherein the following inequality must apply for comparison of the actual external standard time t_{DCF} with the actual internal time t_A :

$$t_{DCF} - t_A < IT * (t_A - t_E),$$

wherein T denotes the tolerance of the internal clock, and

d) Coding the time-stamped digital data.

3. A method according to claim 2, characterised in that a signature for the digital data for time-stamping is obtained, the signature being time-stamped and subsequently coded.

4. A method according to any of the preceding claims, characterised in that the external broadcast or cable signal is the broadcast clock signal DCF77 of the Physikalisch-Technischen Bundesanstalt or the broadcast clock signal from another time transmitter.

5. A method according to any of claims 1 to 3, characterised in that the external broadcast or cable signal is from an independent transmitter, wherein the external broadcast or cable signal contains an authenticating code which sufficiently identifies the transmitter.

6. A method according to claim 5, characterised in that the external broadcast or cable signal is transmitted in coded form.

7. A method according to claim 5 or 6, characterised in that external broadcast or cable signal is transmitted or received at a time which itself is a part of the coding.

8. A method according to any of claims 5-7, characterised in that the external broadcast or cable signal contains true and false information.

9. A method according to any of the preceding claims, characterised in that the external broadcast or cable signal contains information from which the place of reception can be determined.

10. A method according to any of the preceding claims, characterised in that the external broadcast or cable signal is a GPS signal.

11. Apparatus for preparing a time stamp for digital data comprising:

- A receiver for receiving and evaluating an external broadcast or cable signal from an external time source from which the standard time t_{DCF} can be derived,

- An internal clock for generating an internal time

signal t_A ,
 A comparator for comparing the obtained external standard time t_{DCF} with the internal time t_A ,

- A memory containing a latest valid standard time signal t_E and
- A means for time-stamping the digital data if the difference between the internal and the external standard time signal is within a preset tolerance range,

wherein the latest valid standard time signal t_E must satisfy the inequality

$$t_{DCF} > t_E$$

and wherein the following inequality must apply for comparison of the actual external standard time t_{DCF} with the actual internal time t_A :

$$t_{DCF} - t_A < IT * (t_A - t_E),$$

wherein T denotes the tolerance of the internal clock.

12. Apparatus for sealing digital data comprising

- A receiver for receiving and evaluating an external broadcast or cable signal from an external time source from which the standard time t_{DCF} can be derived;
- An internal clock for generating an internal time signal t_A ;
- A comparator for comparing the obtained external standard time t_{DCF} with the internal time t_A ;
- A memory containing a latest valid standard time signal t_E and
- A means for time-stamping the digital data if the difference between the internal and the external standard time signal is within a preset tolerance range,

wherein the latest valid standard time signal t_E must satisfy the inequality

$$t_{DCF} > t_E$$

and wherein the following inequality must apply for comparison of the actual external standard time t_{DCF} with the actual internal time t_A :

$$t_{DCF} - t_A < IT * (t_A - t_E),$$

wherein T denotes the tolerance of the internal clock,

and

a means for coding the time stamped digital data.

13. Apparatus according to claim 11 or 12, characterised in that after positive evaluation of the comparison, the latest valid time signal t_E in the form of the standard time t_{DCF} is stored in the memory and the internal real-time clock is updated.

14. Apparatus according to claim 12 or 13, characterised in that the apparatus comprises a means for preparing a signature for the digital data to be time stamped, wherein the signature is time-stamped and coded.

15. Apparatus according to any of claims 11 to 14, characterised in that the apparatus comprises an authenticating device.

16. Apparatus according to any of claims 11 to 15, characterised in that the apparatus has an identification number which is incorporated in the coding process.

17. Apparatus according to any of claims 11 to 16, characterised in that signal processing in the apparatus is performed by microprocessor components.

18. Apparatus according to any of claims 11 to 17, characterised in that the apparatus is protected against clocking-down.

19. Apparatus according to any of claims 11 to 18, characterised in that the apparatus is integrally cast with its components and is provided with an electromechanical coupling technique.

20. Apparatus according to any of claims 11 to 19, characterised in that the apparatus is disposed on a main computer circuit board or inside a means that can be used for remote data transmission.

21. Apparatus according to any of claims 11 to 19, characterised in that the apparatus is in the form of a PC plug-in card or additional circuit board.

Revendications

1. Procédé pour établir une marque temporelle pour des données numériques, qui comprend les étapes suivantes :

- a) réception et exploitation d'un signal externe, transmis par radio ou par câble, d'une source externe de temps, à partir de laquelle on peut obtenir le temps normal t_{DCF} ,
- b) comparaison du temps normal t_{DCF} déterminé en a) à un signal interne actuel de temps t_A d'une horloge interne,
- c) marquage temporel des données numériques, dans le cas où l'intervalle de temps entre le signal de temps interne et le signal de temps externe se situe à l'intérieur d'une gamme prédéterminée de tolérance,

- le signal de temps normal t_E valable en dernier lieu devant satisfaire à l'inégalité

$$t_{DCF} > t_E$$

et

- l'inégalité suivante devant être valable pour la comparaison du temps normal actuel externe t_{DCF} au temps normal actuel interne t_A :

$$t_{DCF} - t_A < IT * (t_A - t_E)I,$$

T désignant la tolérance de l'horloge interne.

2. Procédé pour sceller des données numériques, qui comprend les étapes suivantes :

- a) réception et exploitation d'un signal externe, transmis par radio ou par câble, d'une source externe de temps, à partir de laquelle on peut obtenir le temps normal t_{DCF} ,
- b) comparaison du temps normal t_{DCF} déterminé en a) à un signal interne actuel de temps t_A d'une horloge interne,
- c) marquage temporel des données numériques, dans le cas où l'intervalle de temps entre le signal de temps interne et le signal de temps externe se situe à l'intérieur d'une gamme prédéterminée de tolérance,

- le signal de temps normal t_E valable en dernier lieu devant satisfaire à l'inégalité

$$t_{DCF} > t_E$$

et

- l'inégalité suivante devant être valable pour la comparaison du temps normal actuel externe t_{DCF} au temps normal actuel interne t_A :

$$t_{DCF} - t_A < IT * (t_A - t_E)I,$$

T désignant la tolérance de l'horloge interne.

- d) codage des données numériques marquées temporellement.

3. Procédé selon la revendication 2, caractérisé en ce qu'un signal des données numériques devant être marquées temporellement est établi, le signal étant marqué temporellement, puis codé.

4. Procédé selon l'une des revendications précédentes, caractérisé en ce qu'on utilise comme signal externe transmis par radio ou par câble le signal d'horloge radio DCF77 du ministère fédéral allemand Physikalisch-Technischer Bundesanstalt ou le signal d'horloge radio d'un autre émetteur de temps.

5. Procédé selon l'une des revendications 1-3, caractérisé en ce que l'émission du signal externe transmis par radio ou par câble est réalisée par un émetteur indépendant, le signal externe transmis par radio ou par câble contenant un code d'authentification, qui identifie d'une manière suffisante l'émetteur.

6. Procédé selon la revendication 5, caractérisé en ce que le signal externe transmis par radio ou par câble est émis sous forme codée.

7. Procédé selon la revendication 5 ou 6, caractérisé en ce que le signal externe transmis par radio ou par câble est émis ou reçu à un instant qui fait lui-même partie du codage.

8. Procédé selon l'une des revendications 1-7, caractérisé en ce que le signal externe transmis par radio ou par câble contient des informations vraies et fausses.

9. Procédé selon l'une des revendications précédentes, caractérisé en ce que le signal externe transmis par radio ou par câble contient des informations, à partir desquelles le lieu de réception peut être déterminé.

10. Procédé selon l'une des revendications précédentes, caractérisé en ce que le signal externe transmis par radio ou par câble est un signal GPS.

11. Dispositif pour établir une marque temporelle pour des données numériques, qui comporte :

- un récepteur pour recevoir et exploiter un signal externe transmis par radio ou par câble, d'une source de temps externe, à partir de laquelle le temps normal t_{DCF} peut être obtenu,
- une horloge interne pour produire un signal de temps interne t_A ,
- un comparateur pour comparer le temps normal externe déterminé t_{DCS} au temps interne t_A ,
- une mémoire, qui contient un signal de temps normal t_E valable en dernier lieu, et
- un moyen de marquage temporel des données numériques dans le cas où l'intervalle de temps entre le signal de temps interne et le signal de temps externe se situe à l'intérieur d'une gamme prédéterminée de tolérance,
- le signal de temps normal t_E valable en dernier lieu devant satisfaire à l'inégalité

$$t_{DCF} > t_E$$

et

- l'inégalité suivante devant être valable pour la comparaison du temps normal actuel externe t_{DCF} au temps normal actuel interne t_A :

$$t_{DCF} - t_A < IT * (t_A - t_E)I,$$

T désignant la tolérance de l'horloge interne.

12. Dispositif pour sceller des données numériques, qui comporte :

- un récepteur pour recevoir et exploiter un signal externe transmis par radio ou par câble, d'une source de temps externe, à partir de laquelle le temps normal t_{DCF} peut être obtenu,
- une horloge interne pour produire un signal de temps interne t_A ,
- un comparateur pour comparer le temps normal externe déterminé t_{DCS} au temps interne t_A ,
- une mémoire, qui contient un signal de temps normal t_E valable en dernier lieu, et
- un moyen de marquage temporel des données numériques dans le cas où l'intervalle de temps entre le signal de temps interne et le signal de temps externe se situe à l'intérieur d'une gamme prédéterminée de tolérance,
- le signal de temps normal t_E valable en dernier lieu devant satisfaire à l'inégalité

et

- l'inégalité suivante devant être valable pour la comparaison du temps normal actuel externe t_{DCF} au temps normal actuel interne t_A :

$$t_{DCF} - t_A < IT * (t_A - t_E)I,$$

T désignant la tolérance de l'horloge interne,

- un moyen pour coder les données numériques marquées temporellement.

13. Dispositif selon l'une des revendications 11 ou 12, caractérisé en ce qu'après une exploitation positive de la comparaison, le temps normal t_{DCF} est mémorisé dans la mémoire en tant que signal de temps t_E valable en dernier lieu, et l'horloge en temps réel est actualisée.

14. Dispositif selon la revendication 12 ou 13, caractérisé en ce que le dispositif comporte un moyen pour établir un signal des données numériques devant être marquées temporellement, le signal étant marqué temporellement et codé.

15. Dispositif selon l'une des revendications 11 à 14, caractérisé en ce que le dispositif comporte un dispositif d'authentification.

16. Dispositif selon l'une des revendications 11 à 15, caractérisé en ce que le dispositif comporte un numéro d'identification, qui est inséré lors du processus de codage.

17. Dispositif selon l'une des revendications 11 à 16, caractérisé en ce que le traitement du signal dans le dispositif est exécuté à l'aide des modules de microprocesseurs.

18. Dispositif selon l'une des revendications 11 à 17, caractérisé en ce que le dispositif est protégé vis-à-vis d'une réduction du cadencement.

19. Dispositif selon l'une des revendications 11 à 18, caractérisé en ce que le dispositif équipé de ses composants est encapsulé et est pourvu d'un système de couplage électromécanique.

20. Dispositif selon l'une des revendications 11 à 19, caractérisé en ce que le dispositif est situé sur une platine principale d'ordinateur ou à l'intérieur d'un appareil exécutant une télétransmission de données.

21. Dispositif selon l'une des revendications 11 à 19,

1999, 2000, 2001, 2002, 2003, 2004, 2005, 2006, 2007, 2008, 2009, 2010, 2011, 2012, 2013, 2014, 2015, 2016, 2017, 2018, 2019, 2020, 2021, 2022, 2023, 2024, 2025, 2026, 2027, 2028, 2029, 2030, 2031, 2032, 2033, 2034, 2035, 2036, 2037, 2038, 2039, 2040, 2041, 2042, 2043, 2044, 2045, 2046, 2047, 2048, 2049, 2050, 2051, 2052, 2053, 2054, 2055, 2056, 2057, 2058, 2059, 2060, 2061, 2062, 2063, 2064, 2065, 2066, 2067, 2068, 2069, 2070, 2071, 2072, 2073, 2074, 2075, 2076, 2077, 2078, 2079, 2080, 2081, 2082, 2083, 2084, 2085, 2086, 2087, 2088, 2089, 2090, 2091, 2092, 2093, 2094, 2095, 2096, 2097, 2098, 2099, 2100, 2101, 2102, 2103, 2104, 2105, 2106, 2107, 2108, 2109, 2110, 2111, 2112, 2113, 2114, 2115, 2116, 2117, 2118, 2119, 2120, 2121, 2122, 2123, 2124, 2125, 2126, 2127, 2128, 2129, 2130, 2131, 2132, 2133, 2134, 2135, 2136, 2137, 2138, 2139, 2140, 2141, 2142, 2143, 2144, 2145, 2146, 2147, 2148, 2149, 2150, 2151, 2152, 2153, 2154, 2155, 2156, 2157, 2158, 2159, 2160, 2161, 2162, 2163, 2164, 2165, 2166, 2167, 2168, 2169, 2170, 2171, 2172, 2173, 2174, 2175, 2176, 2177, 2178, 2179, 2180, 2181, 2182, 2183, 2184, 2185, 2186, 2187, 2188, 2189, 2190, 2191, 2192, 2193, 2194, 2195, 2196, 2197, 2198, 2199, 2200, 2201, 2202, 2203, 2204, 2205, 2206, 2207, 2208, 2209, 2210, 2211, 2212, 2213, 2214, 2215, 2216, 2217, 2218, 2219, 2220, 2221, 2222, 2223, 2224, 2225, 2226, 2227, 2228, 2229, 2230, 2231, 2232, 2233, 2234, 2235, 2236, 2237, 2238, 2239, 2240, 2241, 2242, 2243, 2244, 2245, 2246, 2247, 2248, 2249, 2250, 2251, 2252, 2253, 2254, 2255, 2256, 2257, 2258, 2259, 2260, 2261, 2262, 2263, 2264, 2265, 2266, 2267, 2268, 2269, 2270, 2271, 2272, 2273, 2274, 2275, 2276, 2277, 2278, 2279, 2280, 2281, 2282, 2283, 2284, 2285, 2286, 2287, 2288, 2289, 2290, 2291, 2292, 2293, 2294, 2295, 2296, 2297, 2298, 2299, 2300, 2301, 2302, 2303, 2304, 2305, 2306, 2307, 2308, 2309, 2310, 2311, 2312, 2313, 2314, 2315, 2316, 2317, 2318, 2319, 2320, 2321, 2322, 2323, 2324, 2325, 2326, 2327, 2328, 2329, 2330, 2331, 2332, 2333, 2334, 2335, 2336, 2337, 2338, 2339, 2340, 2341, 2342, 2343, 2344, 2345, 2346, 2347, 2348, 2349, 2350, 2351, 2352, 2353, 2354, 2355, 2356, 2357, 2358, 2359, 2360, 2361, 2362, 2363, 2364, 2365, 2366, 2367, 2368, 2369, 2370, 2371, 2372, 2373, 2374, 2375, 2376, 2377, 2378, 2379, 2380, 2381, 2382, 2383, 2384, 2385, 2386, 2387, 2388, 2389, 2390, 2391, 2392, 2393, 2394, 2395, 2396, 2397, 2398, 2399, 2400, 2401, 2402, 2403, 2404, 2405, 2406, 2407, 2408, 2409, 2410, 2411, 2412, 2413, 2414, 2415, 2416, 2417, 2418, 2419, 2420, 2421, 2422, 2423, 2424, 2425, 2426, 2427, 2428, 2429, 2430, 2431, 2432, 2433, 2434, 2435, 2436, 2437, 2438, 2439, 2440, 2441, 2442, 2443, 2444, 2445, 2446, 2447, 2448, 2449, 2450, 2451, 2452, 2453, 2454, 2455, 2456, 2457, 2458, 2459, 2460, 2461, 2462, 2463, 2464, 2465, 2466, 2467, 2468, 2469, 2470, 2471, 2472, 2473, 2474, 2475, 2476, 2477, 2478, 2479, 2480, 2481, 2482, 2483, 2484, 2485, 2486, 2487, 2488, 2489, 2490, 2491, 2492, 2493, 2494, 2495, 2496, 2497, 2498, 2499, 2500, 2501, 2502, 2503, 2504, 2505, 2506, 2507, 2508, 2509, 2510, 2511, 2512, 2513, 2514, 2515, 2516, 2517, 2518, 2519, 2520, 2521, 2522, 2523, 2524, 2525, 2526, 2527, 2528, 2529, 2530, 2531, 2532, 2533, 2534, 2535, 2536, 2537, 2538, 2539, 2540, 2541, 2542, 2543, 2544, 2545, 2546, 2547, 2548, 2549, 2550, 2551, 2552, 2553, 2554, 2555, 2556, 2557, 2558, 2559, 2560, 2561, 2562, 2563, 2564, 2565, 2566, 2567, 2568, 2569, 2570, 2571, 2572, 2573, 2574, 2575, 2576, 2577, 2578, 2579, 2580, 2581, 2582, 2583, 2584, 2585, 2586, 2587, 2588, 2589, 2590, 2591, 2592, 2593, 2594, 2595, 2596, 2597, 2598, 2599, 2600, 2601, 2602, 2603, 2604, 2605, 2606, 2607, 2608, 2609, 2610, 2611, 2612, 2613, 2614, 2615, 2616, 2617, 2618, 2619, 2620, 2621, 2622, 2623, 2624, 2625, 2626, 2627, 2628, 2629, 2630, 2631, 2632, 2633, 2634, 2635, 2636, 2637, 2638, 2639, 2640, 2641, 2642, 2643, 2644, 2645, 2646, 2647, 2648, 2649, 2650, 2651, 2652, 2653, 2654, 2655, 2656, 2657, 2658, 2659, 2660, 2661, 2662, 2663, 2664, 2665, 2666, 2667, 2668, 2669, 2670, 2671, 2672, 2673, 2674, 2675, 2676, 2677, 2678, 2679, 2680, 26

5. The Commission has also received information from the public that the Commission's decision to grant the license to the applicant was based on the applicant's promise to provide a certain number of jobs to the local community. The Commission has not received any information from the applicant regarding this promise.

10. For a \mathbb{Q} -algebra A , let $\mathcal{A} = \{a \in A : a^2 = 0\}$.
 Suppose \mathcal{A} is not nilpotent. Let $\mathcal{A}^2 = \{a^2 : a \in \mathcal{A}\}$.
 Show that \mathcal{A}^2 is not nilpotent.

SECRET//NOFORN//NF
UNCLASSIFIED//NOFORN

[illegible]

25

30

35

[illegible]

45

50

55

FIG. 1

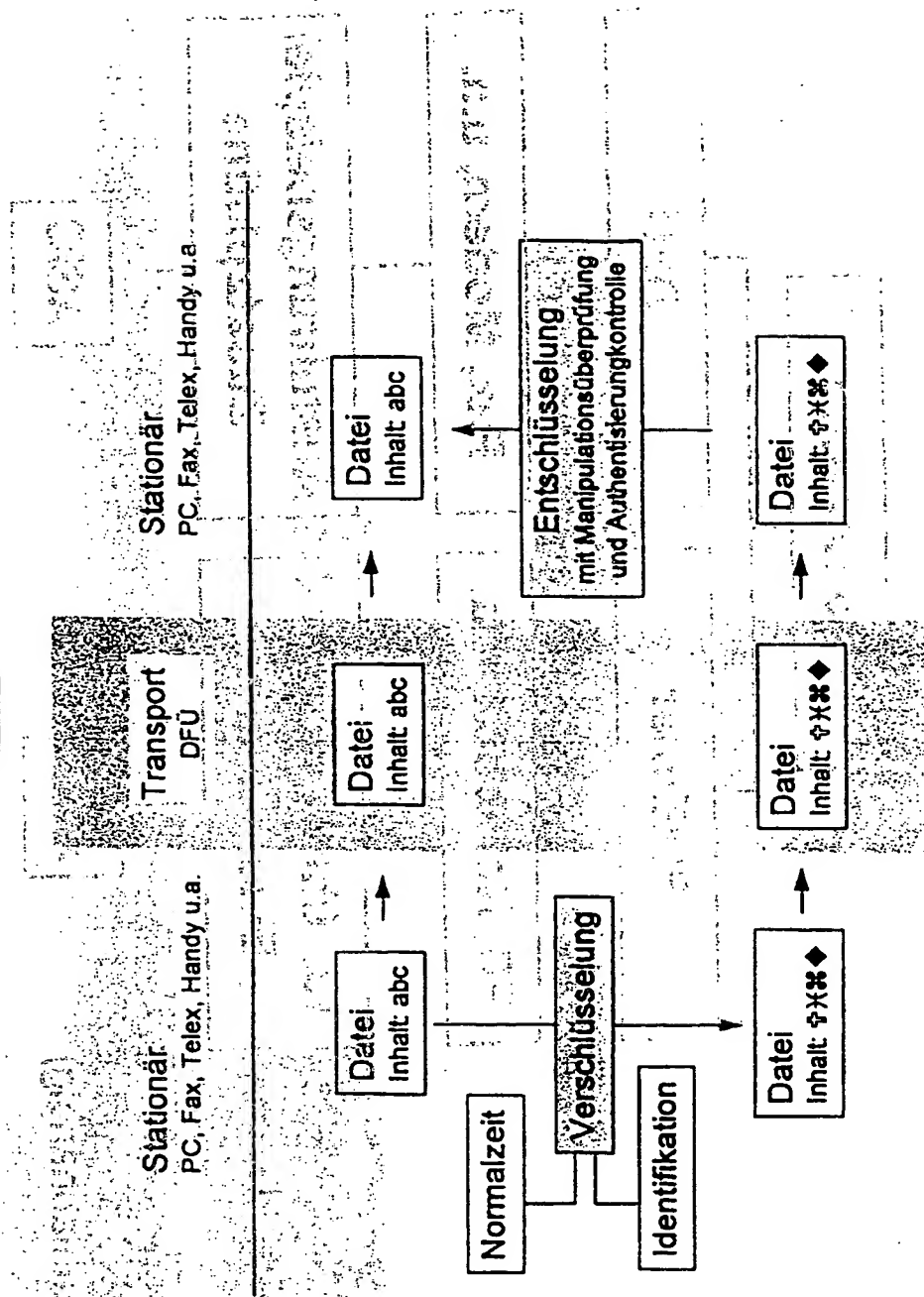


FIG. 2

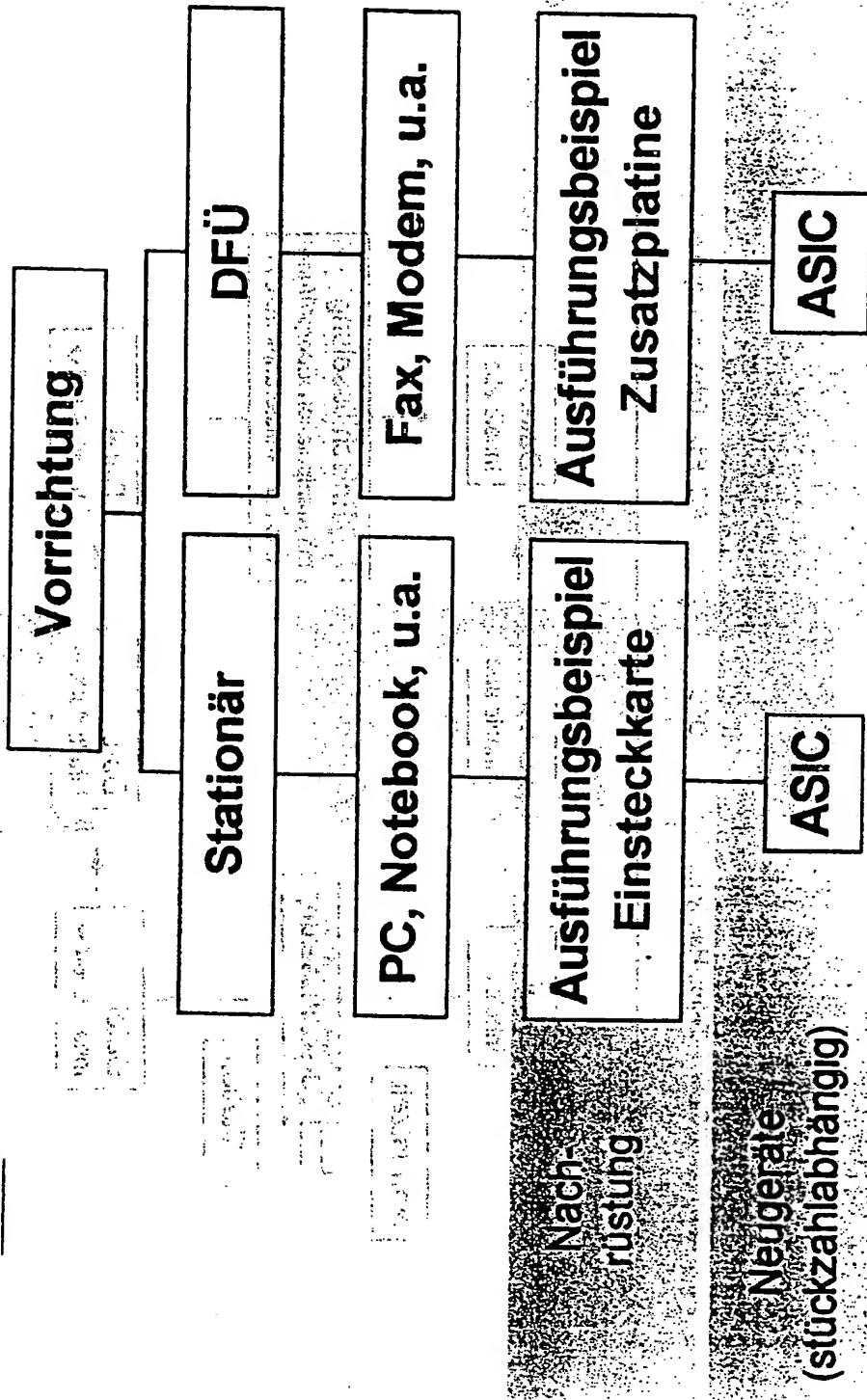
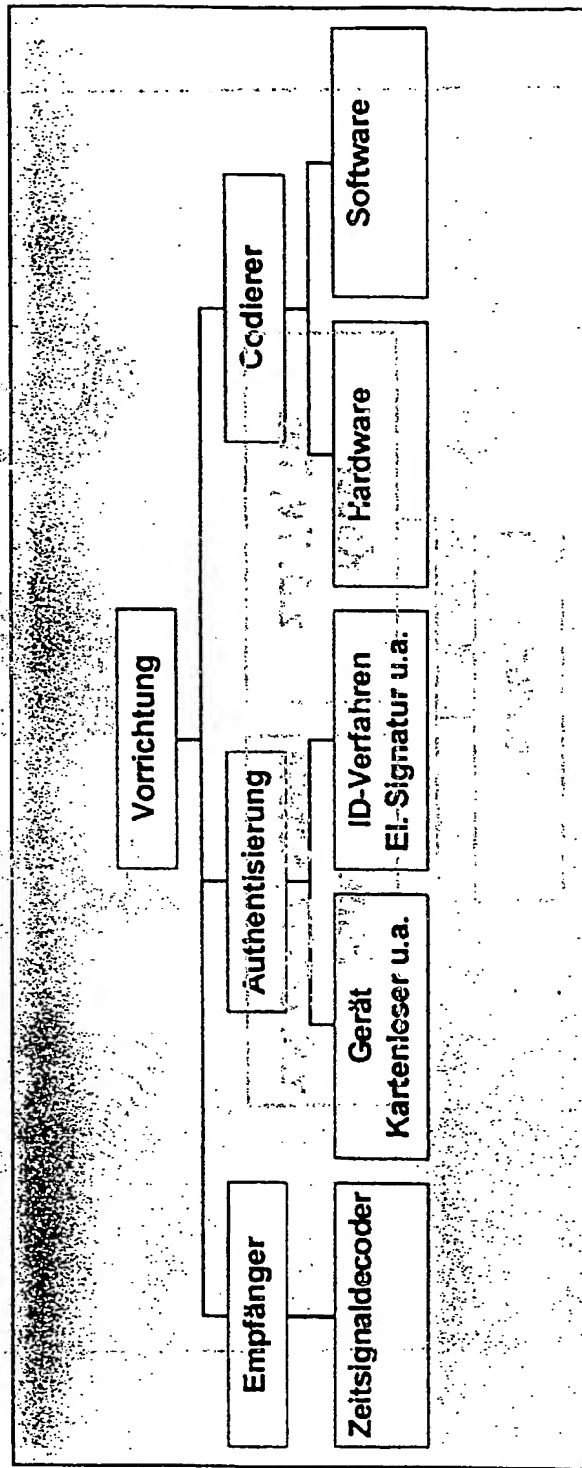


FIG. 3



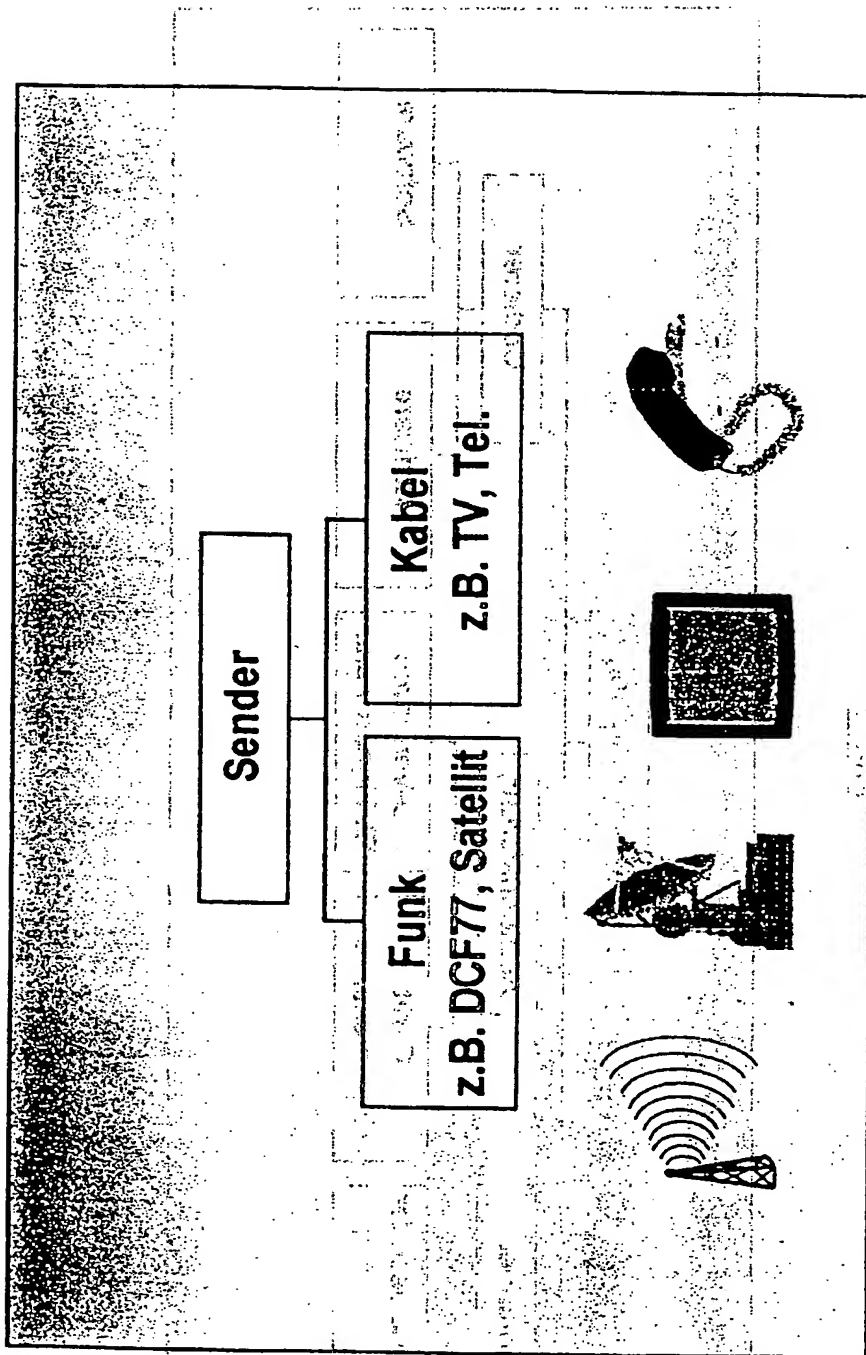


FIG. 4

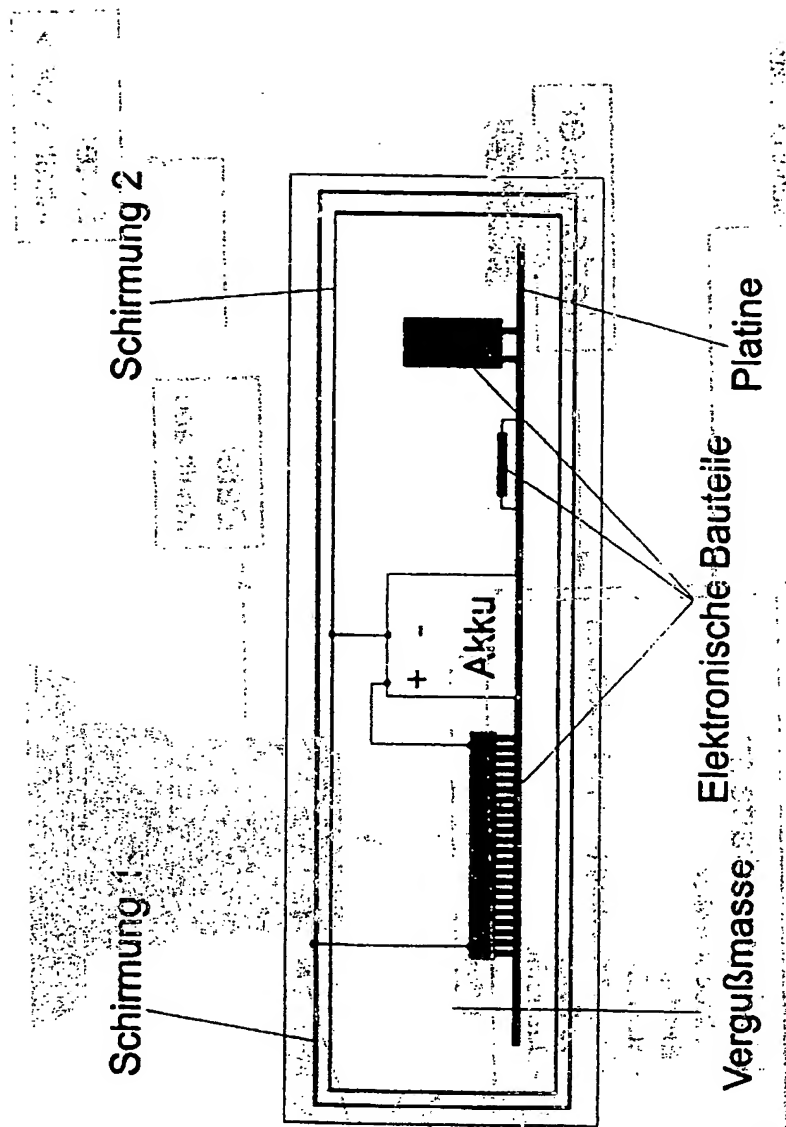


FIG. 5

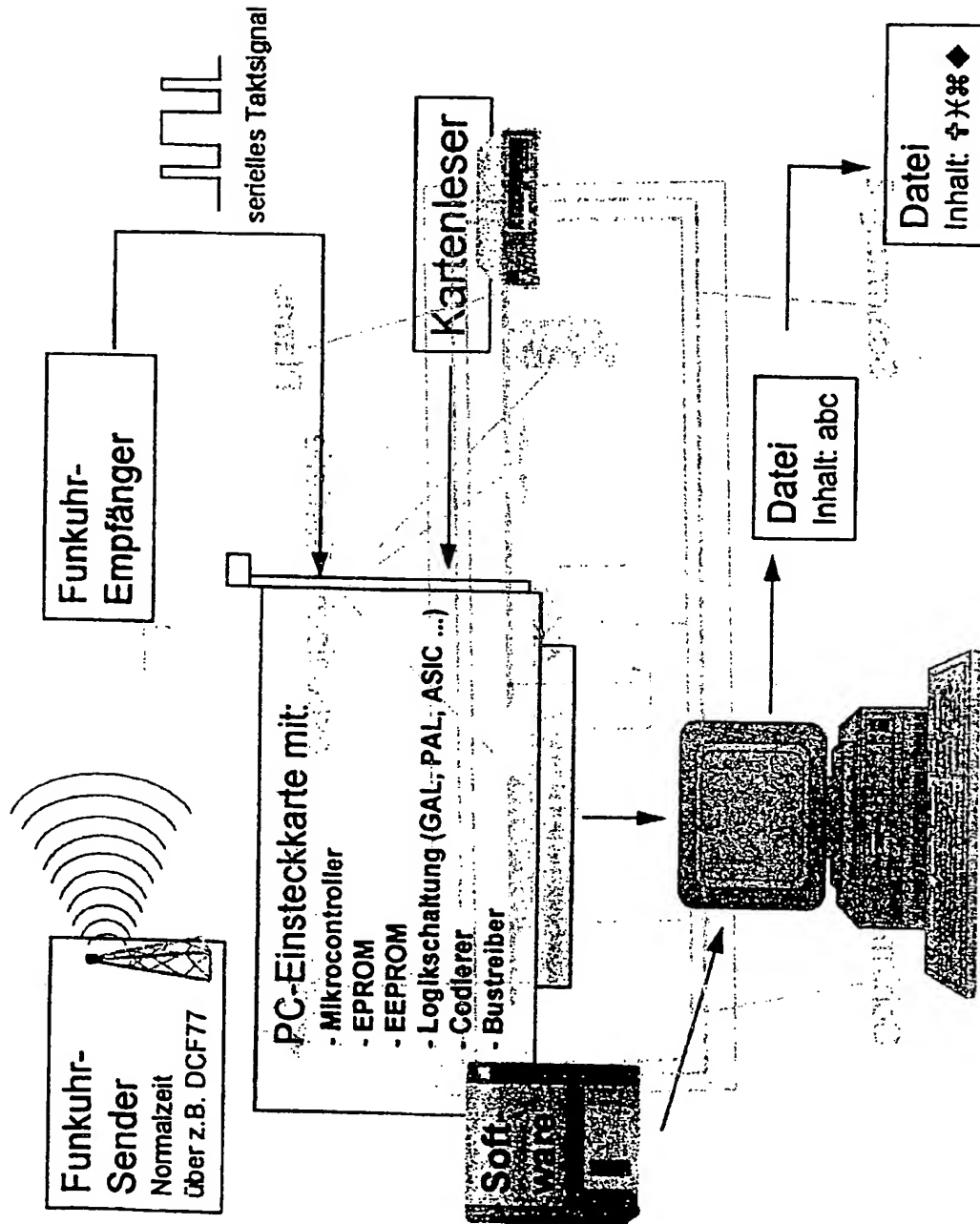


FIG. 6

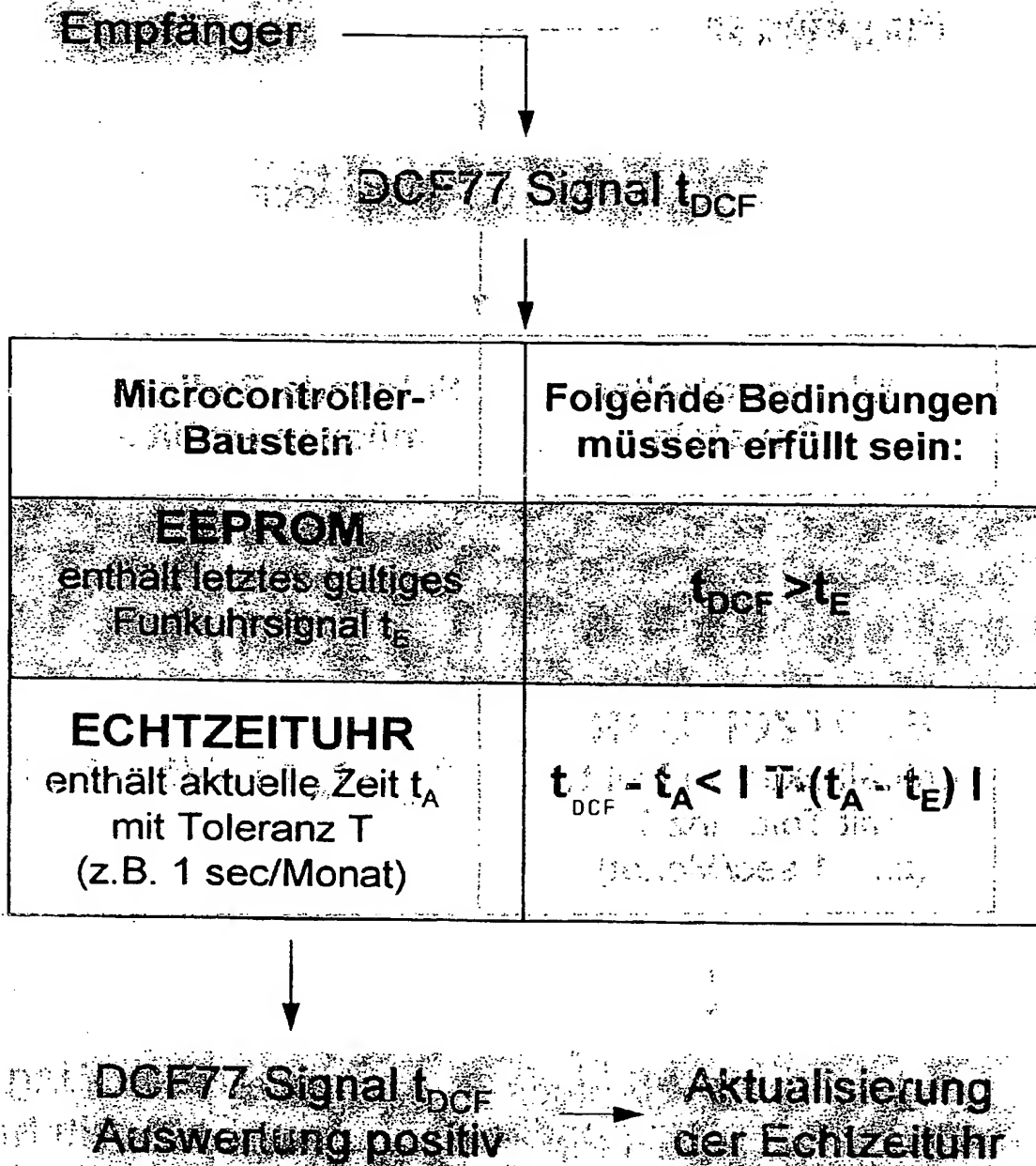


FIG. 7

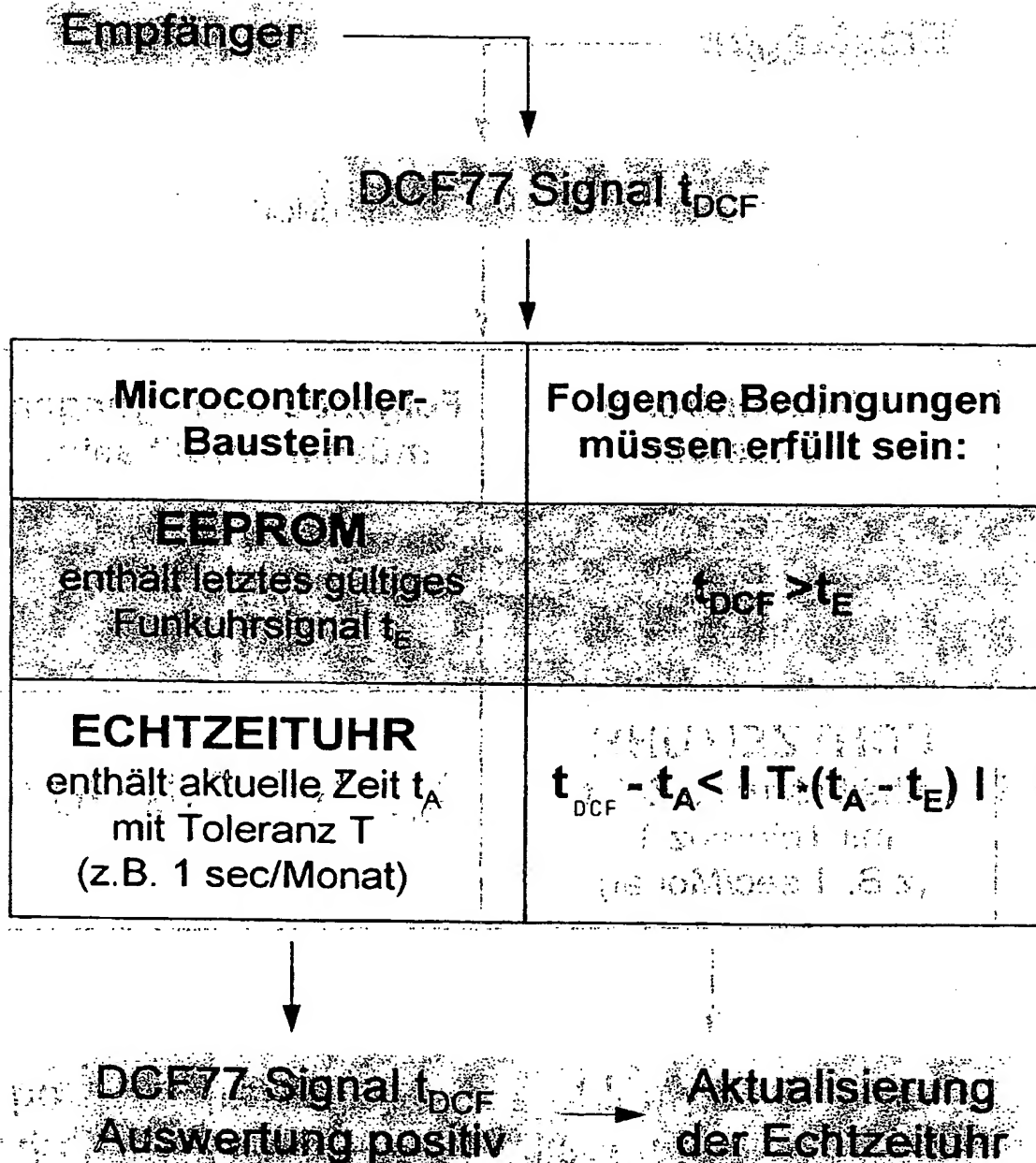


FIG. 7

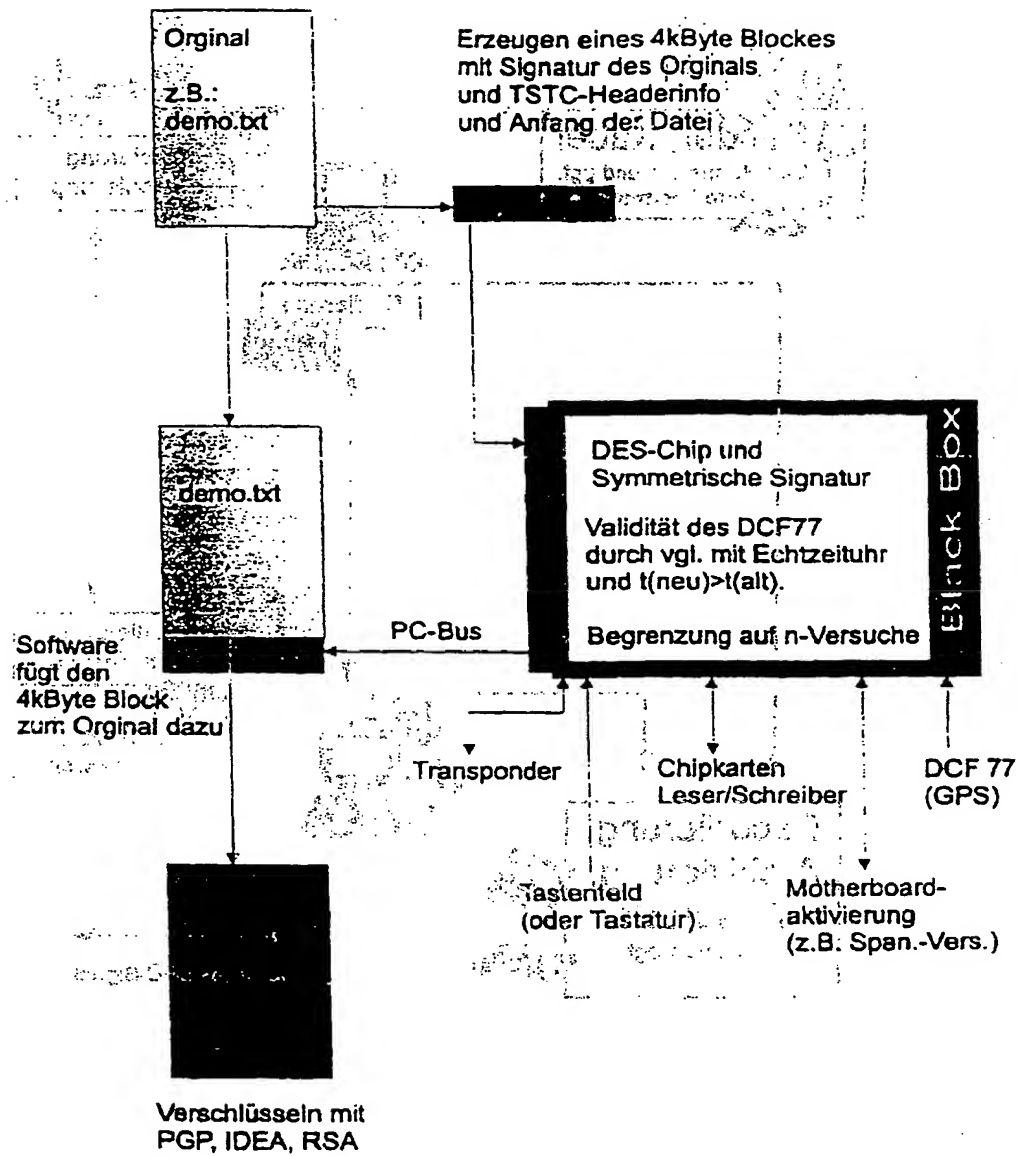


FIG. 8

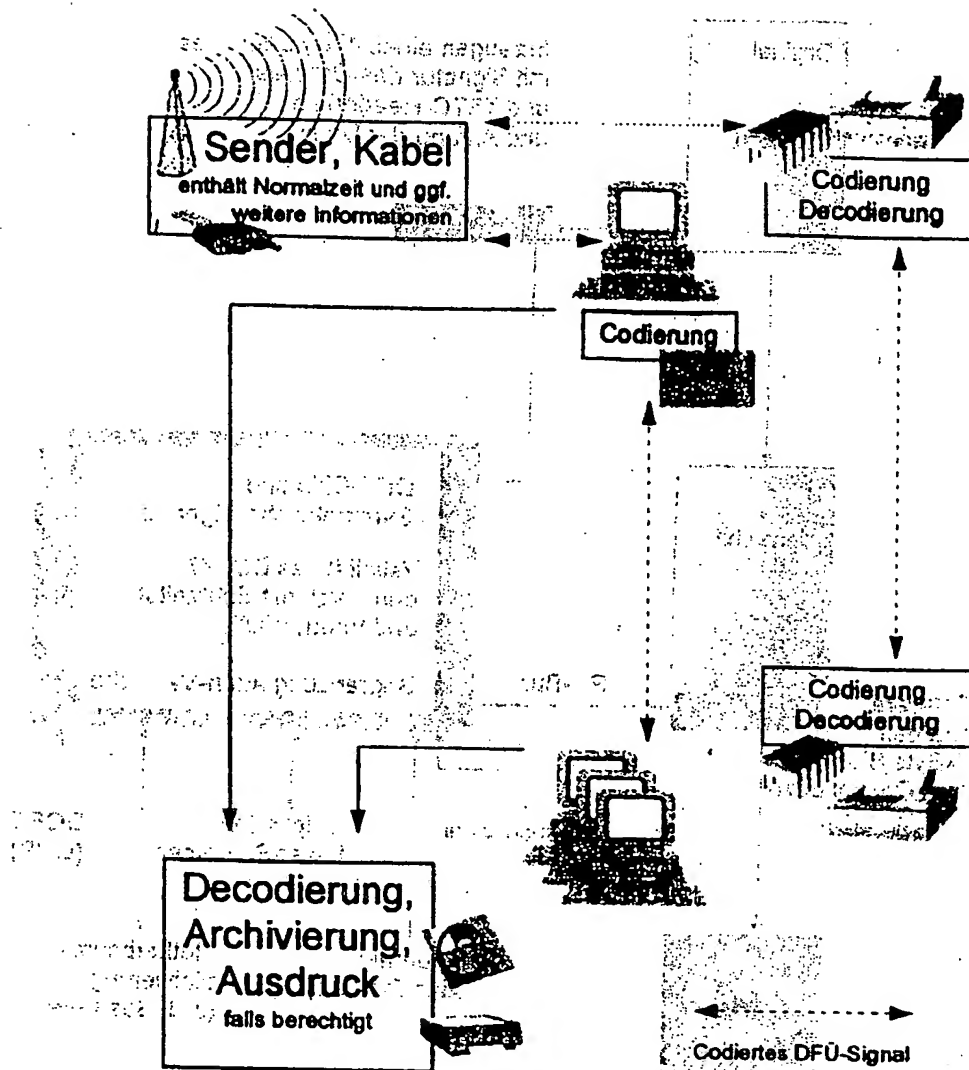


FIG. 9

This Page Blank (uspto)